

# Cohomological framework for contextual quantum computations

Robert Raussendorf

*Department of Physics and Astronomy, University of British Columbia, Vancouver, BC, Canada*

(Dated: April 1, 2016)

We present a cohomological formulation of measurement-based quantum computation (MBQC), employing the notion of a phase function. The phase function describes symmetries of the resource state of the MBQC, specifies the computational output, and acts as a contextuality witness. It is also a topological object, namely a 1-cochain in group cohomology. Non-exactness of the cochain reveals the presence of contextuality, and is a precondition for quantum speedup.

PACS numbers: 03.67.Mn, 03.65.Ud, 03.67.Ac

The Boolean Algebra [1] is at the foundation of all digital classical computation. Is this, when enriched with the superposition principle, the same for quantum computation? Or are there other algebraic structures in Hilbert space that enable quantum algorithms? Any candidate for such a structure must satisfy two criteria: (i) It must specify an input, an output, and a function computed, and (ii) it must be genuinely quantum.

There are indeed examples for such quantum computational structures [2], [3]. The simplest one identified to date is Mermin's star [4]. Its quantumness is revealed through contextuality [4] – [8], an obstruction to describing quantum mechanics in a classical statistical fashion, similar to Bell non-locality [9]. Mermin's star also computes. This is demonstrated by Anders and Browne's contextual 3-qubit measurement-based quantum computation (MBQC) [10], which is based on the state-dependent version of Mermin's star.

In addition to [10] and its numerous cousins, there exists a contextual MBQC with a real application and a super-polynomial (as far as is known) quantum speed-up, namely the MBQC version of the deterministic variant [11] of the 'Discrete Log' quantum algorithm [12], which breaks the Diffie-Hellman key exchange (DES) [13].

These observations prompt the question of how individual examples such as [10] fit into a common framework, and, as a first step, which structural insight is to be gleaned from Mermin's star for computation. Here, we provide answers to these questions, for the model of measurement-based quantum computation [14]. The key element in Mermin's star is its non-trivial cohomology (see below, also [15]). Further, there is a common framework for contextual quantum computations that makes use of the phase function, a topological object known from crystallography in Fourier space [16]–[18].

The phase function enters MBQC through the description of a group of symmetry transformations on the resource state, but it has further computational and physical meaning for MBQC. Namely, it encodes the function computed, up to an additive constant, and it is a witness for contextuality and thus quantumness.

To establish a cohomological framework for MBQC, we combine two links, namely the link between cohomology and contextuality identified by Abramsky and coworkers [15], and the link between contextuality and MBQC [10],

[19]. To make those links match, the Čech cohomology used in [15] is replaced by group cohomology [20], and the model of MBQC is moderately generalized.

This paper is organized as follows. First we describe a generalization of MBQC where the possible inputs form a finite group  $G$ . Then we present the topological formulation of this generalization in terms of a phase function  $\Phi$ , which is a 1-cochain in group cohomology.  $G$ -MBQCs are classified through the second cohomology group of  $G$ , as instances of the group extension problem [20].

We find the following physical and computational manifestations of the topological description: For any phase function  $\Phi$ ,  $d\Phi \neq 0$  is (i) a precondition for the function computed in the  $G$ -MBQC to be non-trivial, and (ii) a witness for contextuality in the quantum computation. Furthermore, (iii) for any given  $G$ -MBQC, we identify a logical contextuality inequality whose maximal violation puts an upper bound on the cost of reproducing the computational output by classical means. Significant speedup thus requires large amounts of contextuality.

*Generalized notion of MBQC.*—We consider the standard setting [14] of MBQC, where the input and the output of the computation are classical. To this setting we apply a generalization and a specialization. The specialization is to temporally flat MBQCs, i.e., all measurement bases are independent of all measurement outcomes. This is a substantial restriction which needs to be lifted in a subsequent more detailed treatment. We also confine to a single output bit, for notational simplicity.

The generalization concerns the set of possible inputs, which is typically a string of bits. Here we assume the inputs to form a finite group  $G$ , Abelian or non-Abelian. The motivation for this generalization is to pinpoint the underlying topological structure. We note that (i) standard MBQC remains a special case, with  $G = \mathbb{Z}_2^m$ ,  $m \in \mathbb{N}$ , and (ii) some structure in the set of inputs is required, for otherwise an unreasonable amount of computational power could be packed into the mapping between inputs and measurement settings; See Appendix A.

We assume that the dimension  $d$  of the underlying Hilbert space  $\mathcal{H}$  is finite, and that all measurable observables have eigenvalues  $\pm 1$  only (they need not be Pauli operators, however). We denote the set of these observables by  $\mathcal{O}_+$ . We also define the enlarged set  $\Omega_+ := \mathcal{O}_+ \cup \{T(g), g \in G\} \cup \{I\}$ , where the observ-

ables  $T(g)$  are those for which the measured eigenvalues  $(-1)^{o(g)}$  provide the computational outputs  $o(g)$ . The set  $\Omega_+$  is labeled by an index set  $\mathcal{A}$ ,  $\Omega_+ = \{T_a, a \in \mathcal{A}\}$ . We require that if  $T_a \in \Omega_+$  then  $-T_a \notin \Omega_+$ .

For the input value being the identity  $e \in G$ , the observables in a reference context  $C(e)$ , with  $[T_a, T_{a'}] = 0$ ,  $\forall T_a, T_{a'} \in C(e)$ , are simultaneously measured on an MBQC resource state  $\rho$ . The corresponding measured eigenvalues  $(-1)^{s(a)}$  are post-processed to infer the eigenvalue  $(-1)^{o(e)}$  of the observable  $T(e) = \prod_{a|T_a \in C(e)} T_a$ . The outcome  $o(e)$  of the MBQC given the input  $e \in G$  is thus related to the measurement outcomes via  $o(e) = \sum_{a|T_a \in C(e)} s(a) \pmod 2$ .

Regarding all input values, we require of  $G$  that it has a projective representation  $u(G)$  acting on  $\mathcal{H}$ . Then, the measurement context for any input  $g \in G$  is

$$C(g) = \{u(g)T_a u(g)^\dagger, T_a \in C(e)\}. \quad (1)$$

The observables  $T(g) := \prod_{a|T_a \in C(g)} T_a$ , with measured eigenvalues  $(-1)^{o(g)}$ , represent the output of the computation. For all  $g \in G$ , the computational output  $o(g)$  is related to the measurement outcomes via

$$o(g) = \sum_{a|T_a \in C(g)} s(a) \pmod 2. \quad (2)$$

This setting we call  $G$ -MBQC.

Above, Eq. (2) relating measurement outcomes to computational output is standard in MBQC [14], but Eq. (1) relating the input of the computation to the measurement settings represents a modification and extension of the original scheme. The latter remains a special case, with  $G = \mathbb{Z}_2^m$ ,  $m \in \mathbb{N}$ ; See Appendix B.

Let's apply the above definitions to the simplest contextual MBQC, the measurement-based OR-gate [10]. We will use this example for illustration throughout. The point about the OR-gate is that it promotes the limited classical control computer in MBQC to classical universality. The resource state is a 3-qubit Greenberger-Horne-Zeilinger state  $|\Psi\rangle$ , with stabilizer relations

$$\begin{aligned} |\Psi\rangle &= X_1 X_2 X_3 |\Psi\rangle = -X_1 Y_2 Y_3 |\Psi\rangle \\ &= -Y_1 X_2 Y_3 |\Psi\rangle = -Y_1 Y_2 X_3 |\Psi\rangle, \end{aligned} \quad (3)$$

and measurement contexts  $C_{00} = \{X_1, X_2, X_3\}$ ,  $C_{01} = \{X_1, Y_2, Y_3\}$ ,  $C_{10} = \{Y_1, X_2, Y_3\}$ ,  $C_{11} = \{Y_1, Y_2, X_3\}$ , for the inputs  $(0, 0), (0, 1), (1, 0), (1, 1) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ . The input group is  $G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \langle g_{01}, g_{10} \rangle$ , with

$$u(g_{01}) = I_1 \otimes A_2 \otimes A_3, \quad u(g_{10}) = A_1 \otimes I_2 \otimes A_3. \quad (4)$$

Therein,  $A := (X + Y)/\sqrt{2}$ , and thus  $AXA^\dagger = Y$  and  $AYA^\dagger = X$ . Hence, Eq. (1) reproduces the above four contexts for the corresponding input values.

To summarize,  $G$ -MBQCs take as input an element  $g$  of a finite input group  $G$ , and are run in three steps. 1) Classical pre-processing. The input  $g \in G$  is converted by the CC into the measurement context  $C(g)$ , cf.

Eq. (1). 2) Quantum part. The observables  $T_a \in C(g)$  are measured, yielding outcomes  $s(a)$ . 3) Classical post-processing. The output  $o(g)$  is obtained from the measurement outcomes  $\{s(a)\}$  via Eq. (2). Comparing with standard MBQC, the CC requires new capability, to accomplish above Step 1.

*Topological formulation of  $G$ -MBQC.*—There exists a group of equivalence transformations changing the set  $\Omega_+$ , namely  $T_a \mapsto T'_a = (-1)^{\mathbf{v}(a)} T_a$ ,  $\forall a \in \mathcal{A}, \forall \mathbf{v} \in V$ , where the phases  $\mathbf{v}(a) \in \mathbb{Z}_2$  are such that they preserve all product relations among commuting observables in  $\Omega_+$ . That is, if  $[T_a, T_b] = 0$  and  $T_c = \pm T_a T_b$  then

$$\mathbf{v}(c) = \mathbf{v}(a) + \mathbf{v}(b) \pmod 2, \quad (5)$$

and  $V$  is the maximal set of such transformations. If  $\mathbf{u}, \mathbf{v} \in V$  then  $\mathbf{u} + \mathbf{v} \in V$ ; hence  $V = \mathbb{Z}_2^m$ ,  $m \in \mathbb{N}$ .

All resource states allowed in  $G$ -MBQC satisfy a symmetry constraint based on a corresponding module  $V$ . We denote by  $\Xi_\rho$  the collection of all expectation values of interest for the given  $G$ -MBQC,  $\Xi_\rho(a) = \langle T_a \rangle_\rho$ ,  $\forall a \in \mathcal{A}$ .  $\Xi_\rho$  may be viewed as a characteristic function, the Fourier transform of a suitably defined quasiprobability function; See Appendix D.

We now define the phase function  $\Phi : G \rightarrow V$ .  $\Phi$  depends on two arguments,  $g \in G$  and  $a \in \mathcal{A}$ ; namely  $\Phi : g \mapsto \Phi_g \in V$ , and  $\Phi_g : a \mapsto \Phi_g(a) \in \mathbb{Z}_2$ . The pair  $(G, \Phi)$  enforces a symmetry constraint on the resource state  $\rho$  of  $G$ -MBQC,

$$\Xi_\rho(ga) = (-1)^{\Phi_g(a)} \Xi_\rho(a). \quad (6)$$

for all  $a \in \mathcal{A}$ , and all  $g \in G$ . We note that this symmetry condition is reminiscent of a corresponding condition on the Fourier density in Fourier space crystallography [17].

How restrictive is Eq. (6)?—First, the GHZ-MBQC Eqs. (3), (4) satisfies it. A corresponding phase function may be worked out from the property  $|GHZ\rangle \sim Y_1 g_{01} |GHZ\rangle \sim Y_2 g_{10} |GHZ\rangle \sim Y_3 g_{11} |GHZ\rangle$ . More generally, Eq. (6) applies to a large class of MBQCs with stabilizer states as resource; See Lemma 2 in Appendix B.

We now discuss the computational and quantum mechanical content of the phase function  $\Phi$ .

(a) *Phase function and computation.* Up to an additive constant, the phase function contains full information about the computational output, as we now explain. For any  $a \in \mathcal{A}$ , the probability  $p_a(s)$  for obtaining the outcome  $s$  in the measurement of  $T_a$  is  $p_a(s) = (1 + (-1)^s \Xi_\rho(a))/2$ , and the probability  $p_{ga}(s')$  for the outcome  $s'$  of  $T_{ga}$  is  $p_{ga}(s') = (1 + (-1)^{s'} \Xi_\rho(ga))/2$ . With the symmetry property Eq. (6) of the resource state  $\rho$ ,  $p_a(s) = p_{ga}(s')$  if the outcomes  $s$  and  $s'$  are related via  $s = s' + \Phi_g(a)$ , for all  $g \in G$ . Now, for any  $g \in G$ , we define the 'intended' outcome  $o(g)$  as the likeliest outcome of the measurement of  $T(g)$ . With the preceding relation, first, the success probability of computation is uniform over  $G$ , and furthermore the output function is

$$o(g) = \Phi_g(b_e) + \text{const.} \pmod 2, \quad (7)$$

where  $\text{const.} = o(e)$ , and  $b_e$  is such that  $T_{b_e} = T(e)$ .

(b) *Phase function and quantumness.* The phase function is a witness for contextuality in the corresponding  $G$ -MBQC. Recall that  $G$  maps  $\mathcal{O}_+$  to itself and  $\Omega_+$  to itself under conjugation. The action of  $G$  on  $\Omega_+$  implies an action of  $G$  on  $\mathcal{A}$ . Namely,  $\forall a \in \mathcal{A}$  and  $\forall g \in G$ ,  $ga$  is defined through  $T_{ga} = u(g)T_a u(g)^\dagger$ . Since the quantum state is not changed under the action of  $G$  (Heisenberg picture), expectation values also transform as  $g : \langle T_a \rangle_\rho \mapsto \langle T_{ga} \rangle_\rho$ , for all  $g \in G$ .

Now consider a non-contextual hidden variable model (ncHVM) with a state space  $\mathcal{S}$  and a consistent value assignment  $s_\nu : \mathcal{A} \rightarrow \mathbb{Z}_2$ ,  $\nu \in \mathcal{S}$ . Under all  $g \in G$ , the assignments  $s_\nu(a)$  transform in the same way as the corresponding expectation values  $\langle T_a \rangle_\rho$ , i.e.,  $g : s_\nu(a) \mapsto s_\nu(ga)$ ,  $\forall g \in G$ ,  $\forall a \in \mathcal{A}$ . Then, the following holds.

**Lemma 1** *If  $s$  is a consistent ncHVM value assignment, then so is  $g(s) := s \circ g^{-1}$ . If  $s$  and  $s'$  are consistent ncHVM value assignments, then there exists a  $\mathbf{v} \in V$  such that  $s' = s + \mathbf{v} \pmod{2}$ .*

The proof of Lemma 1 is given in Appendix C 1.

With Lemma 1, we may introduce phase functions to the classical setting of ncHVMs. Namely, for every consistent value assignment  $s$ , there is a corresponding phase function  $\Phi : G \rightarrow V$  such that

$$s(ga) = s(a) + \Phi_g(a) \pmod{2}, \forall a \in \mathcal{A}, \forall g \in G. \quad (8)$$

Since  $s((gh)a) = s(g(h(a)))$ , Eq. (8) holds for a given  $\Phi$  if and only if the group compatibility condition [17]

$$\Phi_{gh}(a) = \Phi_h(a) + \Phi_g(ha) \pmod{2} \quad (9)$$

is satisfied for all  $g, h \in G$  and all  $a \in \mathcal{A}$ .

The group compatibility condition can be stated in topological terms [18]. Namely, in group cohomology [20] a  $k$ -cochain is a map  $\varphi^k : \mathcal{G}^k \rightarrow M$ , where  $\mathcal{G}$  is a group and  $M$  is a module on which  $\mathcal{G}$  acts. Now,  $V$  is a module, and furthermore, the action of  $G$  on  $\mathcal{A}$  implies an action on  $V$ , namely  $(g(\mathbf{v}))(a) = \mathbf{v}(g^{-1}a)$ , for all  $a \in \mathcal{A}$ ; See Lemma 6 in Appendix D 2. Therefore, the phase function  $\Phi : G \rightarrow V$  is a 1-cochain. It has a coboundary  $d\Phi : G \times G \rightarrow V$ , given by  $(d\Phi)_{g,h}(a) := \Phi_g(ha) + \Phi_h(a) - \Phi_{gh}(a) \pmod{2}$ . By comparison with Eq. (9), we find that the group compatibility condition on phase functions  $\Phi^{(cl)}$  describing ncHVMs has a topological interpretation,

$$d\Phi^{(cl)} = 0. \quad (10)$$

This condition is in general incompatible with quantum mechanics, as the following result shows.

**Proposition 1** *Consider a  $G$ -MBQC  $\mathcal{M}$  that computes a function  $o : G \rightarrow \mathbb{Z}_2$ . If for all phase functions  $\Phi$  satisfying the output relation Eq. (7) it holds that  $d\Phi \neq 0$ , then  $\mathcal{M}$  is contextual.*

*Proof of Proposition 1.* Assume the given  $G$ -MBQC is non-contextual. Then there exists a consistent ncHVM value assignment  $s$  that reproduces the function  $o$ ; i.e., for  $b_e$  such that  $T_{b_e} = T(e)$ ,

$$s(gb_e) = o(g), \forall g \in G. \quad (11)$$

This assignment  $s$  defines a phase function  $\Phi^{(s)}$  via Eq. (8),  $\Phi_g^{(s)}(a) := s(ga) - s(a) \pmod{2}$ ,  $\forall a \in \mathcal{A}$ ,  $\forall g \in G$ .  $\Phi^{(s)}$  satisfies group compatibility Eq. (9),  $d\Phi^{(s)} = 0$ . With Eq. (11), it also satisfies the output relation Eq. (7),  $o(g) = s(gb_e) = \Phi_g^{(s)}(b_e) + o(e) \pmod{2}$ .  $\square$

Prop. 1 provides symmetry-based proofs for contextuality of  $G$ -MBQCs; also see [21]. In many instances it can be shown that (i) linearity Eq. (5) of  $\Phi$ , (ii) the output relation Eq. (7), and (iii)  $d\Phi = 0$  are incompatible. With Prop. 1 contextuality then follows.

We illustrate this fact with a symmetry based contextuality proof for the familiar setting of the state-dependent Mermin star [4]. We consider the input group element  $g = g_{01}$  of Eq. (4), which acts on  $\mathcal{O}_+$  as  $X_1 \circlearrowleft$ ,  $Y_1 \circlearrowleft$ ,  $X_2 \leftrightarrow Y_2$ ,  $X_3 \leftrightarrow Y_3$ . Further, be  $a(X_1)$  such that  $T_{a(X_1)} = X_1$ , etc. The 3-qubit GHZ state appearing in Mermin's star has the stabilizer relations Eq. (3), and thus, with Eq. (8),

$$\Phi_g(a_{XXX}) = 1, \Phi_g(a_{YXY}) = 0. \quad (12)$$

Since  $\Phi_g \in V$ , by Eq. (5),

$$\begin{aligned} \Phi_g(a_{XXX}) &= \Phi_g(a_{X_1}) + \Phi_g(a_{X_2}) + \Phi_g(a_{X_3}), \\ \Phi_g(a_{YXY}) &= \Phi_g(a_{Y_1}) + \Phi_g(a_{X_2}) + \Phi_g(a_{Y_3}), \end{aligned} \quad (13)$$

where addition is mod 2. Combining Eqs. (12) and (13),

$$1 = \Phi_g(a_{X_1}) + \Phi_g(a_{X_3}) + \Phi_g(a_{Y_1}) + \Phi_g(a_{Y_3}), \quad (14)$$

with  $g = g_{01}$ . The r.h.s. of Eq. (14) is a 2-coboundary,

$$1 = (d\Phi)_{g_{10}, g_{01}}(a_{X_1}) + (d\Phi)_{g_{01}, g_{10}}(a_{X_1}) + (d\Phi)_{g_{01}, g_{01}}(a_{X_3}).$$

Therefore,  $d\Phi \neq 0$  for all phase functions  $\Phi$  that satisfy Eq. (12), and contextuality follows with Prop. 1.  $\square$

The relation between the present symmetry based and Mermin's parity based contextuality proofs [4] is, for the general case, discussed in Appendix C 2.

As the above example shows, the quantum mechanical phase function defined through the symmetry constraint Eq. (6) on  $G$ -MBQC resource states evades the group compatibility condition, unlike in the crystallography scenario [17]. With Eq. (6) we have  $(-1)^{\Phi_{gh}(a)} \Xi_\rho(a) = \Xi_\rho((gh)a) = \Xi_\rho(g(h(a))) = (-1)^{\Phi_g(ha) + \Phi_h(a)} \Xi_\rho(a)$ . This can be satisfied in two ways; either by the group compatibility condition Eq. (9), or by  $\Xi_\rho(a) = 0$ .

(c) *Phase function and computation.* There is a connection between exactness of  $\Phi$  and efficient classical simulability of the output function  $o$ .

**Proposition 2** Assume that the classical control computer (CC) of  $G$ -MBQC has a memory of  $|\mathcal{O}_+| \times |R|$  bits, where  $R$  is a set of generators of  $G$ . This memory is addressable by pairs  $(a, g)$ , where  $T_a \in \mathcal{O}_+$  and  $g \in R$ . Then, the CC is capable of computing any function  $o$  specified through Eq. (7) by an exact phase function  $\Phi$ ,  $d\Phi = 0$ , without any quantum resources.

*Remark:* If the CC has access to a memory of size  $|\Omega_+|$ , then it can compute any function  $o$  without quantum resources. However, typically,  $|\mathcal{O}_+| \times |R| \ll |\Omega_+|$ . For example, in standard MBQC,  $|\Omega_+ \setminus \mathcal{O}_+| = 2^m$ ,  $|\mathcal{O}_+| = 2n$ , and  $|R| = m$ , where  $m$  is the number of input bits and  $n$  the number of qubits in the cluster state. For efficient such computations,  $n = \text{Poly}(m)$ . The assumption on memory in Prop. 2 is thus that the memory is small.

*Proof of Proposition 2.* The memory cells  $(a, g)$  are assumed to be initialized with the values  $\Phi_a(g)$ , for all  $g \in R$  and all  $a$  with  $T_a \in \mathcal{O}_+$ ; and  $g$  is given as a sequence of generators,  $g = g_k g_{k-1} \dots g_2 g_1$ . Denote  $g(i) := g_i g_{i-1} \dots g_2 g_1$ . By group compatibility Eq. (9),  $\Phi_g(b_e) = \sum_{i=1}^k \Phi_{g_i}(g(i-1)b_e) \bmod 2$ .

The CC can compute  $\Phi_g(b_e)$ , and hence  $o(g)$ , if it can compute all  $\Phi_{g_i}(g(i-1)b_e)$ . By Eq. (5),  $\Phi_{g_i}(g(i-1)b_e) = \sum_{a|T_a \in C(g(i-1))} \Phi_{g_i}(a) \bmod 2$ . The CC has the capability to compute  $a \mapsto g(a)$  (cf. Step 1 of the  $G$ -MBQC procedure) and to add mod 2 (cf. Step 3), hence can evaluate this sum.  $\square$

(d) *Contextuality and speedup.* In view of the contextual 3-qubit MBQC [10] executing an OR-gate, one may ask “What is contextual about an OR-gate?”. A first answer to this question would be that, of course, there is nothing contextual about an OR-gate per se, only one of its physical realizations—the MBQC—is contextual.

But we can say more. For every  $G$ -MBQC, there is a non-contextuality inequality whose maximal violation puts an upper bound on the computational cost of evaluating the  $G$ -MBQC output function by classical means. Therefore, a significant violation of this inequality is required for quantum speedup.

The quantity  $W(o)_\rho := \sum_{g \in G} (1 + (-1)^{o(g)} \langle T(g) \rangle_\rho) / 2$  is a contextuality witnesses. The maximum value allowed by quantum mechanics,  $W(o)_{\rho, \max} = |G|$ , is reached for deterministic  $G$ -MBQCs. Be  $s : \mathcal{A} \rightarrow \mathbb{Z}_2$  an internally consistent, non-contextual value assignment, and  $\mathcal{S}$  the set of all such assignments. Any  $s$  induces a function  $o_s$  via  $o_s(g) = s(gb_e)$ , for all  $g \in G$ , where  $b_e \in \mathcal{A}$  is such that  $T_{b_e} = T(e)$ . The maximum value  $W(o)_{HVM, \max} = |G| - \Delta(o)$  for an ncHVM with deterministic value assignments is therefore given by

$$\Delta(o) = \min_{s \in \mathcal{S}} (\text{wt}(o \oplus o_s)), \quad (15)$$

where  $\text{wt}(r)$  is the Hamming weight of a function  $r : G \rightarrow \mathbb{Z}_2$ . If no consistent non-contextual value assignment reproducing the function  $o$  exists, then  $\Delta(o) > 0$ . This is a logical non-contextuality inequality [22].

**Proposition 3** The classical computational cost  $C_{\text{class}}$  of reducing the evaluation of a function  $o : G \rightarrow \mathbb{Z}_2$  to the evaluation of a trivial function  $o'$ , induced via Eq. (7) by a phase function  $\Phi$  with  $d\Phi = 0$ , is bounded by the maximum violation of the logical non-contextuality inequality Eq. (15),  $C_{\text{class}} \leq \Delta(o)$ .

Taken together with Prop. 2, this result establishes that a large amount of contextuality is necessary for quantum speedup. It is thus a contextuality counterpart to corresponding results [23],[24] for entanglement, and [25] for the negativity of Wigner functions. Also see [26], [27] for the role of contextuality.

*Proof of Proposition 3.* We establish the upper bound by explicit construction of an algorithm that matches it. Be  $s$  a consistent non-contextual value assignment, with  $o'(g) := s(gb_e)$  where  $b_e$  is such that  $T_{b_e} = T(e)$ , that maximizes the r.h.s. of Eq. (15). We assume the set  $\tilde{G} := \{g \in G | o'(g) \neq o(g)\}$  is given in table form. To classically evaluate the function  $o$  in question, for any input  $g \in G$ , check membership in  $\tilde{G}$ . If  $g \in \tilde{G}$ , output  $o'(g) \oplus 1$ , otherwise output  $o'(g)$ . This reduces the evaluation of the function  $o$  to the evaluation of  $o'$ . Since  $|\tilde{G}| = \Delta(o)$ , the operational cost of sifting through the list  $\tilde{G}$  (the memory cost of storing  $\tilde{G}$ ) is bounded by (given by)  $\Delta(o)$ .

It remains to show that  $o'$  is induced via Eq. (7) by a cohomologically trivial phase function  $\Phi$ , i.e.  $d\Phi \equiv 0$ . Define  $\Phi_g(a) := s(ga) - s(a) \bmod 2$ . Then,  $(d\Phi)_{g,h}(a) = (s(gha) - s(ha)) + (s(ha) - s(a)) - (s(gha) - s(a)) \bmod 2 = 0$ . Further,  $o'(g) = s(gb_e) = \Phi_g(b_e) + s(b_e) \bmod 2 = \Phi_g(b_e) + o(e) \bmod 2$ , as required by Eq. (7).  $\square$

(e) *Cohomological classification of  $G$ -MBQCs.* Given the input group  $G$  and the set  $\Omega_+$  of observables, the corresponding temporally flat  $G$ -MBQCs are classified by the solutions to the group extension problem [20].

For each temporally flat  $G$ -MBQC, there is a group  $E$  of symmetry transformations which fix the characteristic function  $\Xi_\rho$  of resource state  $\rho$ .  $E$  has a normal subgroup  $N$  to be defined, and the input group  $G$  as the quotient  $E/N$ . The injection  $\eta : G \hookrightarrow E$  is such that the characteristic function  $\Xi_\sigma$  of a general quantum state  $\sigma$  is, for all  $g \in G$ , transformed according to

$$(\eta(g)(\Xi_\sigma))(a) = (-1)^{\Phi_g(a)} \Xi_\sigma(ga), \quad \forall a \in \mathcal{A}. \quad (16)$$

With Eq. (6), the characteristic function  $\Xi_\rho$  of a resource state  $\rho$  is thus preserved for all  $g \in G$ , as required.

$N$  is a subgroup of  $V$  such that  $\forall n \in N$ ,  $n(a) = 0$ ,  $\forall a | T_a \in \Omega_+ \setminus \mathcal{O}_+$ , and  $n \in N$  acts on  $\Xi$  via  $(n(\Xi))(a) := (-1)^{n(a)} \Xi(a)$ . By construction,  $N$  leaves the computational output unaffected. It is no further restriction to assume that it also leaves the characteristic function  $\Xi_\rho$  of a resource state  $\rho$  unaffected, for if not we may always replace  $\Xi_\rho \mapsto \Xi_{\rho'}$ , with  $\Xi_{\rho'}(a) = \frac{1}{|N|} \sum_{n \in N} (-1)^{n(a)} \Xi_\rho(a)$ ,  $\forall a \in \mathcal{A}$ . Thus,

$$E = \{\eta(g)n | n \in N, g \in G\} \quad (17)$$

is a set of symmetry transformations on  $\Xi_\rho$ . In Appendix E we show that (i)  $E$  is a group, (ii)  $N$  is a normal subgroup of  $E$  and (iii)  $G \cong E/N$ . Given  $N$  and  $G$ , what can  $E$  be?—This is the group extension problem.

What is left unspecified about  $E$  given the fragments  $G$  and  $N$  is the product  $\eta(g)\eta(h)$ . Since group compatibility may fail in the quantum scenario,  $\eta$  is not guaranteed to be a homomorphism. But since all  $\eta(g)$  are symmetry transformations, it holds that  $\eta(g)\eta(h) = \eta(gh)\lambda(g, h)$ ,  $\forall g, h \in G$ , where  $\lambda : G \times G \rightarrow N$ . Therein,  $\lambda$  is fully specified by the phase function  $\Phi$ .

Thus, given the input group  $G$  and the set of observables  $\Omega_+$ , but not  $\Phi/\rho$ , the subgroup  $N$  is fully specified but  $E$  isn't. The possible groups  $E$  are classified by the elements of  $H^2(G, N)$  [20]. They correspond to inequivalent phase functions  $\Phi$ , which in turn lead to different output functions  $o$  and different resource states  $\rho$ .

*Conclusion.*—We have presented a generalization of measurement-based quantum computation in which the classical inputs form a finite group  $G$ , and have provided a topological classification of such  $G$ -MBQCs by group extensions. Therein, the symmetry of the resource state is described by a phase function, which is a 1-cochain

in group cohomology. We have described computational and physical ramifications of this topological fact. For any given  $G$ -MBQC, non-exactness of the phase function is a witness of quantumness in the form of contextuality, and a precondition for speedup.

The next step suggested by this work is to extend the cohomological framework to  $G$ -MBQCs with proper temporal order. Further, group cohomology has also reached the subject of MBQC in a different vein, namely through the notion of ‘computational phases of matter’ [28]–[31] within the paradigm of symmetry-protected topological order [32]. In view of the striking formal resemblance, is there a physical relation?

From a broad perspective, the present work raises the following question: “Is there a quantum computational paradigm that relates to contextuality in the same way as ‘quantum parallelism’ [33] relates to superposition and interference?” Here we have provided an algebraic framework within which any emerging contender may be examined and utilized.

*Acknowledgments.* The author thanks Dan Browne and Cihan Okay for discussions. This work has been funded by NSERC and Cifar.

- 
- [1] George Boole, *An Investigation of the Laws of Thought*, Prometheus Books (2003) [1854].
  - [2] D. Aharonov, V. Jones, Z. Landau, *Algorithmica* **55**, 395 (2009).
  - [3] J. Bermejo-Vega, K.C. Zatloukal, arXiv:1511.08506.
  - [4] N. D. Mermin, *Rev. Mod. Phys.* **65**, 803 (1993).
  - [5] S. Kochen and E.P. Specker, *J. Math. Mech.* **17**, 59 (1967).
  - [6] S. Abramsky, A. Brandenburger, *New J. Phys.* **13**, 113036 (2011).
  - [7] A. Cabello, S. Severini, A. Winter, *Phys. Rev. Lett.* **112**, 040401 (2014).
  - [8] A. Acín, T. Fritz, A. Leverrier, A. Belén Sainz, arXiv:1212.4084.
  - [9] J.S. Bell, *Rev. Mod. Phys.* **38**, 447 (1966).
  - [10] J. Anders and D.E. Browne, *Phys. Rev. Lett.* **102**, 050502 (2009).
  - [11] M. Mosca and C. Zalka, arXiv:quant-ph/0301093.
  - [12] P. Shor, *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM (IEEE Press, New York, 1994), p. 124.
  - [13] W. Diffie, M. Hellman, *IEEE Transactions on Information Theory* **22**, 644 (1976).
  - [14] R. Raussendorf and H.J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).
  - [15] S. Abramsky, Shane Mansfield and Rui Soares Barbosa, *EPTCS* **95**, 1 (2012).
  - [16] A. Bienenstock and E.P. Ewald, *Acta Crystallogr.* **15**, 1253 (1962).
  - [17] N.D. Mermin, *Rev. Mod. Phys.* **64**, 3 (1992).
  - [18] D.A. Rabson, J.F. Huesman, and B.N. Fisher, *Found. Phys.* **33**, 1769 (2003).
  - [19] R. Raussendorf, *Phys. Rev. A* **88**, 022322 (2013).
  - [20] A. Adem and R.J. Milgram, *Cohomology of finite groups*, Springer, Berlin Heidelberg (1994).
  - [21] J. Lawrence, *Phys. Rev. A* **89**, 012105 (2014).
  - [22] L. Hardy, *Phys. Lett. A* **161**, 21 (1991).
  - [23] G. Vidal, *Phys. Rev. Lett.* **91**, 147902 (2003).
  - [24] M. Van den Nest, W. Dür, G. Vidal, H. J. Briegel, *Phys. Rev. A* **75**, 012337 (2007).
  - [25] Hakop Pashayan, Joel J. Wallman, Stephen D. Bartlett, *Phys. Rev. Lett.* **115**, 070501 (2015).
  - [26] M. Howard, J.J. Wallman, V. Veitch, J. Emerson, *Nature (London)* **510**, 351 (2014).
  - [27] N. Delfosse, P. Allard Guerin, J. Bian, R. Raussendorf, *Phys. Rev. X* **5**, 021003 (2015).
  - [28] A. Miyake, *Phys. Rev. Lett.* **105**, 040501 (2010).
  - [29] D.V. Else, I. Schwarz, S.D. Bartlett, and A.C. Doherty, *Phys. Rev. Lett.* **108**, 240505 (2012).
  - [30] J. Miller and A. Miyake, *Phys. Rev. Lett.* **114**, 120506 (2015).
  - [31] A. Prakash and T.-C. Wei, *Phys. Rev. A* **92**, 022310 (2015).
  - [32] X. Chen, Z.-C. Gu, and X.-G. Wen, *Phys. Rev. B* **83**, 035107 (2011).
  - [33] R. Cleve, A. Ekert, C. Macchiavello and M. Mosca, *quant-ph/9708016* (1997).

## Appendix A: The need for structure in the input set

If we merely require that the set of input values forms a set with no additional structure, then there is plenty of flexibility in assigning measurement contexts to input values, and this proves to be problematic. Namely, a large amount of computational power can be packed into the relation between inputs and measurement contexts.

The sets  $C(\mathbf{i})$  of measured observables are labeled by the input value  $\mathbf{i}$ . If  $\tau : \mathbf{i} \mapsto C(\mathbf{i})$ , for all input values  $\mathbf{i} \in G$ , is a valid assignment of computational inputs to the contexts, then so is  $\tau_P : \mathbf{i} \mapsto C(P\mathbf{i})$ , where  $P$  is an arbitrary permutation of the elements in  $G$ . Thus, if a given MBQC can realize a function  $o : G \rightarrow \mathbb{Z}_2^m$ , with  $m \in \mathbb{N}$ , it can also realize the function  $o_P = o \circ P$ .

This is an unsatisfactory state of affairs, as the following example illustrates. Consider first an MBQC with one input and one output bit,  $|\Psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$ ,  $C(0) = \{X_1, X_2\}$ ,  $C(1) = \{Y_1, Y_2\}$ , and  $o = s_1 \oplus s_2$ . The computed function is the identity,  $o(i) = i$ . Now tensor this computation  $m$  times with itself, resulting in an MBQC that evaluates the identity function on  $m$ -bit-strings. Nothing is being computed so far. However, by the above freedom in assigning contexts to input values, we can also compute any invertible function  $P$  on  $G = \mathbb{Z}_2^m$ . Then we can also compute any Boolean function  $o : \mathbb{Z}_2^{m-1} \rightarrow \mathbb{Z}_2$ , since for any such function  $o(\mathbf{i})$ , the  $m$ -bit function  $\mathbf{y}(\mathbf{i}, j) := (\mathbf{i}, j \oplus o(\mathbf{i}))$  is invertible, and  $\mathbf{y}(\mathbf{i}, 0) = (\mathbf{i}, o(\mathbf{i}))$ .

Thus, complete freedom in assigning inputs to contexts gives the power of efficiently computing any Boolean function, which is unreasonable. In addition, note that the quantum part of this MBQC is near trivial. The above example illustrates that the freedom in assigning measurement contexts to input values must be constrained.

## Appendix B: Standard MBQC is in $G$ -MBQC

To demonstrate that standard MBQC [RB] is contained in the generalized framework presented here, we have to show that the classical side-processing in standard MBQC is a special case of the classical side processing here and in standard MBQC are the same, cf. Eq. (2) and [RB]. The difference arises in the preprocessing.

To begin, we note that in both standard MBQC and the present generalization the input specifies the measured observables. In the present setting, this proceeds by the action of an input group on a reference context of measurable observables, see Eq. (1). In the standard setting, no such group action is made explicit. But it is nonetheless there, as we now show.

In the standard setting [RB] of MBQC, a measurement context is associated with a bit string  $\mathbf{i} \in \mathbb{Z}_2^m$  as follows. For each qubit location  $k$ ,  $k = 1, \dots, n$ , there is a flag  $q_k \in$

$\mathbb{Z}_2$  that decides which one of two possible observables,

$$O_k[q_k] = \cos \varphi X_k + (-1)^{q_k} \sin \varphi Y_k, \quad (\text{B1})$$

is going to be measured. We may assemble the flags  $q_k$  in a vector  $\mathbf{q} = (q_1, q_2, \dots, q_n)$ . In this notation, for the special case of temporally flat MBQC considered here, the relation between the input  $\mathbf{i}$  and the vector  $\mathbf{q}$  specifying the measurement setting is linear,

$$\mathbf{q} = Q\mathbf{i} \pmod{2},$$

with  $Q$  a binary-valued matrix. We now note that for the observables in Eq. (B1) it holds that

$$X_k O_k[0] X_k^\dagger = O_k[1] \quad \text{and} \quad X_k O_k[1] X_k^\dagger = O_k[0].$$

There is thus a homomorphism  $g$  from  $\{\mathbf{i}\} = \mathbb{Z}_2^m$  into the  $n$ -qubit Pauli group  $\mathcal{P}_n$ ,

$$\mathbf{i} \mapsto g(\mathbf{i}) := \bigotimes_{l=1}^n (X_l)^{[Q\mathbf{i}]_l},$$

with the property that  $O_k[q_k(\mathbf{i})] = g(\mathbf{i}) O_k[0] g(\mathbf{i})^\dagger$ . The pre-processing in standard MBQC is thus a special case of the generalized setting discussed here. Namely, the input group is  $G = \mathbb{Z}_2^m$  and has a unitary representation  $u(G) = \{g(\mathbf{i}), \mathbf{i} \in \mathbb{Z}_2^m\}$ . The reference context associated with the input  $g = I$  is  $\{O_k[0], k = 1, \dots, n\}$ .

Another question that arises is whether the resource states of MBQC, typically cluster states or, more generally stabilizer states, naturally satisfy the symmetry constraint Eq. (6). This can only hold when the success probability is uniform over all inputs. As for the reverse direction, we have the following Lemma.

**Lemma 2** *If the success probability of MBQC with an input group  $G$  is uniform over  $G$  and the resource state  $|\Psi\rangle$  is a stabilizer state with no single qubit disentangled, then  $|\Psi\rangle$  satisfies the invariance condition Eq. (6).*

*Proof of Lemma 2.* We subdivide the set  $\mathcal{A}$  into three subsets, namely  $\mathcal{A} = \{0\} \cup \mathcal{A}_M \cup \mathcal{A}_{\text{out}}$ , where  $0 \in \mathcal{A}$  is such that  $T_0 = I$ ,  $\mathcal{A}_M := \{a \in \mathcal{A} | T_a \in \mathcal{O}_+\}$  and  $\mathcal{A}_{\text{out}} = \{a \in \mathcal{A} | \exists g \in G \text{ s.th. } T_a = T(g)\}$ .

Case 1:  $\{0\} \subset \mathcal{A}$ . With  $I = I \cdot I$  and linearity of  $\mathbf{v}$ , for all  $\mathbf{v} \in V$ , it holds that  $\mathbf{v}(0) = \mathbf{v}(0) + \mathbf{v}(0) \pmod{2} = 0$ . Since  $\Phi_g \in V$  by definition,  $\Phi_g(0) = 0$  for all  $g \in G$ . Further,  $\langle T_0 \rangle_\sigma = \langle I \rangle_\sigma = 1$  for all normalized quantum states  $\sigma$ . Eq. (6) is thus satisfied for  $0 \in \mathcal{A}$ , for all  $g \in G$ .

Case 2:  $\mathcal{A}_{\text{out}} \subset \mathcal{A}$ . Recall that  $b_e \in \mathcal{A}_{\text{out}}$  is such that  $T_{b_e} = T(e)$ , with  $e$  the identity in  $G$ . Since for all  $g \in G$ ,  $o(g)$  is by definition the outcome with the larger probability, it holds that  $(-1)^{o(g)} \langle T_{gb_e} \rangle_\rho \geq 0$ . With the assumption of uniform success probability, it further holds that  $(-1)^{o(g)} \langle T_{gb_e} \rangle_\rho = (-1)^{o(e)} \langle T_{b_e} \rangle_\rho$ ,  $\forall g \in G$ . With Eq. (7), we thus find that

$$\langle T_{gb_e} \rangle_\rho = (-1)^{\Phi_g(b_e)} \langle T_{b_e} \rangle_\rho, \quad \forall g \in G, \quad (\text{B2})$$

which is a special case of the desired relation in which  $\mathcal{A}_{\text{out}} \ni a = b_e$ . By construction of  $\mathcal{A}_{\text{out}}$ , for all  $a \in \mathcal{A}_{\text{out}}$  there exists a  $h \in G$  such that  $a = hb_e$ . Now, substituting  $g \mapsto gh$  in Eq. (B2), we obtain

$$\begin{aligned}\langle T_{ga} \rangle_\rho &= (-1)^{\Phi_{gh}(b_e)} \langle T_{b_e} \rangle_\rho \\ &= (-1)^{\Phi_h(b_e) + \Phi_g(a)} \langle T_{b_e} \rangle_\rho \\ &= (-1)^{\Phi_g(a)} \langle T_a \rangle_\rho.\end{aligned}$$

Therein, we have used the group compatibility condition Eq. (9) in the second line, and Eq. (B2) in the third. Eq. (6) is thus satisfied for all  $a \in \mathcal{A}_{\text{out}}$ .

Case 3:  $\mathcal{A}_M \subset \mathcal{A}$ . In standard MBQC, all  $T_a$  with  $a \in \mathcal{A}_M$  are local, and of form Eq. (B1). Since, by assumption, no qubit in the resource stabilizer state  $|\Psi\rangle$  is disentangled from the rest, for every qubit  $k = 1, \dots, n$  there is a stabilizer operator  $S$  of  $|\Psi\rangle$  such that  $S|_k = Z_k$ , and hence  $O_k[q]S = -SO_k[q]$ , and  $\langle \Psi | O_k[q] | \Psi \rangle = 0$ ,  $\forall k$ ,  $\forall q$ . Thus, Eq. (6) holds trivially for all  $a \in \mathcal{A}_M$ . Hence it holds for all  $a \in \mathcal{A}$ .  $\square$

## Appendix C: More on contextuality

### 1. Proof of Lemma 1

*Proof of Lemma 1.* Regarding the first statement, denote by  $\mathcal{C}$  the set of all product constraints among commuting observables in  $\Omega_+$ . Since  $u(g)$  is unitary for all  $g \in G$ , conjugation by  $u(g)$  of any such constraint leads another valid product constraint,  $\mathcal{C} \mapsto g(\mathcal{C})$ . If  $s$  is a consistent non-contextual value assignment satisfying the constraints  $\mathcal{C}$ , then,  $\forall g \in G$ ,  $s' := g(s) = s \circ g^{-1}$  is a consistent value assignment for the constraints  $g(\mathcal{C})$ . Further,  $G$  maps  $\Omega$  onto itself under conjugation, and therefore  $g(\mathcal{C}) = \mathcal{C}$ ,  $\forall g \in G$ . Hence,  $s'$  is also a consistent non-contextual value assignment for  $\mathcal{C}$ .

Regarding the second statement, let  $s(\cdot)$  and  $s'(\cdot)$  be two consistent non-contextual value assignments. Then, the following two relations simultaneously hold for all  $a, b, c \in \mathcal{A}$  with  $[T_a, T_b] = 0$  and  $T_c = \pm T_a T_b$ .

$$\begin{aligned}(-1)^{s(c)} T_c &= (-1)^{s(a)} T_a (-1)^{s(c)} T_b, \\ (-1)^{s'(c)} T_c &= (-1)^{s'(a)} T_a (-1)^{s'(c)} T_b.\end{aligned}$$

Therefore, by multiplying the above equalities,

$$(s \oplus s')(c) = (s \oplus s')(a) \oplus (s \oplus s')(b),$$

for all  $a, b, c \in \mathcal{A}$  such that  $[T_a, T_b] = 0$  and  $T_c = \pm T_a T_b$ . Since, by definition,  $V$  is the module of all functions satisfying these relations, it follows that  $s \oplus s' \in V$ .  $\square$

### 2. The relation between symmetry-based and parity-based contextuality proofs

To explain the relation between the present symmetry-based contextuality proofs and Mermin's parity-based

proofs [DM], we first revisit the state-dependent Mermin star discussed in the main text. There is an alternative symmetry-based proof. Namely, we may assume that  $\Phi_g$  in Eq. (14) derives from a consistent value assignment  $s$  via Eq. (8). Then,

$$\begin{aligned}1 &= (s(a_{X_1}) - s(a_{X_1})) + (s(a_{X_3}) - s(a_{Y_3})) + \\ &\quad + (s(a_{Y_1}) - s(a_{Y_1})) + (s(a_{Y_3}) - s(a_{X_3})) \pmod{2} \\ &= 0.\end{aligned}$$

Contradiction. Hence no consistent assignment exists.  $\square$

This proof is closer to Mermin's original proof than the proof presented in the main text. However, like [JL], it is based on a symmetry transformation, which Mermin's proof is not.

Below we explain the relation between the symmetry-based and parity-based contextuality proofs. This relation proceeds via the state-independent version of symmetry-based contextuality proofs, which we have not discussed yet.

For the state independent scenario, we introduce a symmetry group  $\mathcal{G}$  larger than  $G$ ,  $G \subset \mathcal{G}$ . It is based on a set of observables  $\Omega := \{\pm T_a, T_a \in \Omega_+\}$ .  $\mathcal{G}$  has a projective representation  $u(\mathcal{G})$  that maps  $\Omega$  onto itself under conjugation (but it does not necessarily map  $\Omega_+$  to itself). The transformation behaviour under  $\mathcal{G}$  is

$$u(h)T_a u(h)^\dagger = (-1)^{\tilde{\Phi}_h(a)} T_{ha}, \quad \forall h \in \mathcal{G}, \forall a \in \mathcal{A} \quad (\text{C1})$$

where the generalized phase function is a map  $\tilde{\Phi} : \mathcal{A} \rightarrow \tilde{V} = \text{span}(\{\tilde{\Phi}_h, h \in \mathcal{G}\})$ . Note that the space  $\tilde{V}$  into which  $\tilde{\Phi}$  maps is constructed in a different manner from how  $V$  was constructed. As a consequence, the  $\tilde{\Phi}_h \in \tilde{V}$  do not need to satisfy the linearity requirement Eq. (5) imposed on the original phase function  $\Phi$ .

*Transformation of value assignments  $s$ .* In a hidden variable model describing the given physical situation, we require the value assignments  $s : \mathcal{A} \rightarrow \mathbb{Z}_2$  to transform under all  $h \in \mathcal{G}$  in such a way as to match the transformation of the quantum-mechanical expectation values. With the transformation for observables, since the state  $\rho$  doesn't change (Heisenberg picture), the expectation values transform as  $\langle T_a \rangle_\rho \mapsto \langle T'_a \rangle_\rho = (-1)^{\tilde{\Phi}_h(a)} \langle T_{ha} \rangle_\rho$ . Hence, if a consistent value assignment  $s$  exists, it transforms under  $h \in \mathcal{G}$  as

$$s(a) \mapsto s'(a) = s(ha) + \tilde{\Phi}(ha) \pmod{2}. \quad (\text{C2})$$

*Transformation of constraints.* The set  $\mathcal{C}$  of product constraints among commuting observables in  $\Omega$  transforms as

$$\mathcal{G} : \mathcal{C} \rightarrow \mathcal{C}.$$

The proof is the same as for the first statement in Lemma 1. Note that the argument therein does not require  $G$  to map  $\Omega_+$  to  $\Omega_+$  (even though it does), but works for all groups that map  $\Omega$  to  $\Omega$  by unitary transformations. Therefore, the following statement holds.

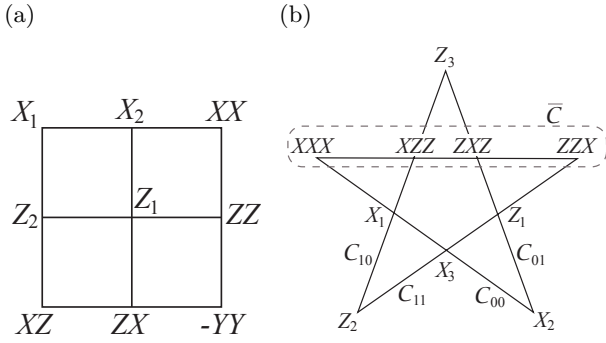


FIG. 1: Mermin's square and star.

**Lemma 3** *If  $s : \mathcal{A} \rightarrow \mathbb{Z}_2$  is a consistent value assignment, then so is  $s' : \mathcal{A} \rightarrow \mathbb{Z}_2$  as given by Eq. (C2), for every  $h \in \mathcal{G}$ .*

*Symmetry-based proofs of contextuality.* Starting from the assumption that a consistent non-contextual value assignment  $s$  exists, Lemma 3 shows how to construct further such assignments  $s'$ . By Lemma 1, for any pair  $(s, s')$  of assignments so constructed, it must hold that  $s - s' \bmod 2 \in V$ . However, in certain situations it can be shown that this is impossible, whatever consistent assignment  $s$  one starts out with. The assumption of the existence of a consistent values assignment  $s$  is thus proven wrong in those cases.

We illustrate the proof technique first in an example, and then discuss the general case. Finally we explain the connection with state-independent parity proofs of contextuality [DM].

*Example 1: Mermin's square.* In this example,  $\Omega_+$  is the set of all observables appearing in Mermin's square (See Fig. 1a),

$$\Omega_+ = \{I, X_1, X_2, X_1 X_2, Z_1, Z_2, Z_1 Z_2, X_1 Z_2, Z_1 X_2, Y_1 Y_2\},$$

and  $\mathcal{A}$  is the corresponding index set.

Assume that a consistent non-contextual value assignment  $s$  exists,  $\mathcal{S} \neq \emptyset$ , and consider the quantities

$$\eta = \sum_{a \in \mathcal{A}} s(a) \bmod 2, \quad s. \quad (\text{C3})$$

Now, for any  $h \in \mathcal{G}$ , consider the transformed quantity  $\eta' = \sum_{a \in \mathcal{A}} s'(a)$ . Using Eq. (C2), and  $h(\mathcal{A}) = \mathcal{A}$ ,

$$\eta' = \eta + \sum_{a \in \mathcal{A}} \tilde{\Phi}_h(a) \bmod 2. \quad (\text{C4})$$

On the other hand, by Lemma 3,  $s'$  is also a valid non-contextual value assignment. Thus, applying Lemma 1 to  $\eta'$ , for every  $h \in \mathcal{G}$  exists a  $\mathbf{v}_h \in V$  such that

$$\eta' = \eta + \sum_{a \in \mathcal{A}} \mathbf{v}_h(a) \bmod 2 = \eta \bmod 2. \quad (\text{C5})$$

The last equality holds because, by construction of Mermin's square,  $\forall \mathbf{v} \in V$  the Hamming weight of  $\mathbf{v}$  is even.

Now we choose a specific element of  $\mathcal{G}$ , namely the Hadamard gate  $H_1$  on the first qubit. Since  $H_1 Y_1 Y_2 H_1^\dagger = -Y_1 Y_2$ , it holds that  $\tilde{\Phi}_{H_1}(a_{YY}) = 1$ . All other values of  $\tilde{\Phi}_{H_1}(a)$ ,  $a \in \mathcal{A} \setminus \{a_{YY}\}$  vanish. Thus,  $\sum_{a \in \mathcal{A}} \tilde{\Phi}_{H_1}(a) \bmod 2 = 1$ . Now comparing Eqs. (C4) and (C5) for the case of  $h = H_1$ , we find

$$\eta + 1 = \eta \bmod 2.$$

Contradiction. Hence, no consistent value assignment  $s$  exists.  $\square$

*Remark:* In the above proof, although we dropped the linearity requirement Eq. (5) from  $\tilde{\Phi}$ , linearity sneaked back in when invoking Lemma 1 to arrive at Eq. (C5).

*General method.* Here we show how to construct symmetry-based contextuality proofs in the general scenario. Suppose there exists an assignment  $s$  of values to all observables in  $\Omega_+$ . We may list these values in a vector  $\mathbf{s}$ , which, according to Eq. (C2), then transforms under any  $h \in \mathcal{G}$  as

$$\mathcal{G} \ni h : \mathbf{s} \mapsto \mathbf{s}' = P_h \mathbf{s} + \mathbf{v}_h \bmod 2, \quad (\text{C6})$$

where  $P_h$  is a permutation matrix, and  $\mathbf{v}_h$  a suitable offset vector. The value assignments  $\mathbf{s}$  and  $\mathbf{s}'$  need to satisfy the same set of linear constraints,

$$K \mathbf{s} \bmod 2 = \mathbf{c} = K \mathbf{s}' \bmod 2,$$

where  $K$  is the constraint matrix with its rows labeled by constraints and its columns labeled by the elements of  $\mathcal{A}$ . Combining the two above equations, we find that

$$K(I - P_h) \mathbf{s} = K \mathbf{v}_h \bmod 2, \quad \forall h \in \mathcal{G}. \quad (\text{C7})$$

If we can find a vector  $\mathbf{a}^T$  such that

$$\mathbf{a}^T K(I - P_h) \bmod 2 = \mathbf{0}^T, \quad \text{and} \quad (\text{C8a})$$

$$\mathbf{a}^T K \mathbf{v}_h \bmod 2 \neq 0, \quad (\text{C8b})$$

this immediately leads to a contradiction in Eq. (C7).

*Connection with Mermin's original parity proofs.* The above contextuality proof and Mermin's original parity proof [DM] are not the same, because Mermin's proof is about the inconsistency of assignments, and the present proof about the inconsistency of the transformation behaviour of assignments. Nonetheless, both proofs employ the same type of algebraic contradiction.

To see this, we revisit the linear system of equations on which Mermin's proof is built (also see [LS]),

$$K \mathbf{s} \bmod 2 = \mathbf{u}. \quad (\text{C9})$$

The goal is to find a vector  $\mathbf{b}$  such that (i)  $\mathbf{b}^T K = \mathbf{0} \bmod 2$ , and (ii)  $\mathbf{b}^T \mathbf{u} \bmod 2 \neq 0$ . Multiplying Eq. (C9) with any such  $\mathbf{b}^T$  immediately leads the contradiction with every noncontextual HVM.



With an eye on the symmetry-based proof displayed in Eq. (C7), we note that the group  $\mathcal{G}$ , by construction, does not only act on the value assignments, but also on the constraints. Therefore, for each  $h \in \mathcal{G}$  there exists a matrix  $P'_h$  such that  $KP_h = P'_h K$ . Now using this in Eq. (C7), we obtain the noncontextual HVM constraint

$$(I - P'_h)K\mathbf{s} = K\mathbf{v}_h \pmod{2}, \forall h \in \mathcal{G}.$$

Therefore, the parity proof based on Eq. (C9) and the symmetry-based proof Eq. (C7) exploit the same algebraic contradiction whenever  $\mathbf{b}^T = \mathbf{a}^T(I - P'_h) \pmod{2}$ . This is possible if  $\mathbf{b} \in \text{Im}(I - P'_h)^T$  for some  $h \in \mathcal{G}$ . Mermin's parity proof method is thus stronger than the present symmetry based proof: Every symmetry-based proof implies a Mermin-type parity proof, but not the other way around.

### 3. No state-independent contextuality in $G$ -MBQC

The set  $\Omega_+$  is constructed such that it is mapped onto itself under conjugation by  $G$ , i.e.,

$$u(g)T_a u(g)^\dagger \in \Omega_+, \forall g \in G, \forall T_a \in \Omega_+. \quad (\text{C10})$$

This property has the following implication with respect to contextuality.

**Lemma 4** *If the pair  $(\Omega_+, G)$  satisfies Eq. (C10), then no symmetry-based state-independent contextuality proof can be based on it.*

*Proof of Lemma 4.* Eq. (C10) implies that in Eq. (C6)  $\mathbf{v}_g = \mathbf{0}$ , for all  $g \in G$ . Thus, the relation Eq. (C8b) needed for a symmetry-based contextuality proof cannot be satisfied for any  $\mathbf{a}$ . Hence, no symmetry-based contextuality proof exists for the pair  $(\Omega_+, G)$ .  $\square$

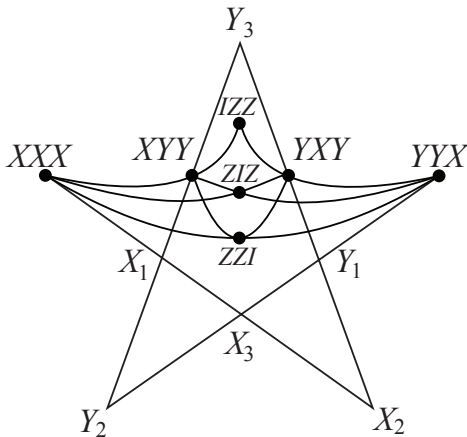


FIG. 2: Dressed Mermin star.

*Example 2: Dressed Mermin star.* By Lemma 4, the above symmetry-based state-dependent contextuality proofs for Mermin's star have no state-independent counterpart. However, we may “dress” Mermin's star in such a way that Eq. (C10) no longer holds, and Lemma 4 is circumvented.

The dressed Mermin star is shown in Fig. 2. Therein, the set  $\Omega_+$  used in Mermin's original star (see Fig. 1b) is enlarged to

$$\Omega_+ \longrightarrow \Omega'_+ = \Omega_+ \cup \{Z_1 Z_2, Z_1 Z_3, Z_2 Z_3\}.$$

The new observables are dependent on the set of observables  $\{Y_1 Y_2 X_3, Y_1 X_2 Y_3, X_1 Y_2 Y_3\}$  which are already in  $\Omega_+$ . Now,  $G$  does not map  $\Omega'_+$  to itself under conjugation. For example,

$$A_1 A_2 Z_1 Z_3 (A_1 A_2)^\dagger = -Z_1 Z_3. \quad (\text{C11})$$

We now show that, in consequence, the pair  $(\Omega'_+, G)$  does lead to a state-independent symmetry-based contextuality proof. Following the argument in Appendix C 2, we choose a subset  $\Upsilon$  of  $\Omega'_+$ ,

$$\Upsilon = \{X_1, X_3, Y_1, Y_3, X_1 Y_2 Y_3, Y_1 X_2 Y_3, Z_2 Z_3\},$$

and consider the linear combination

$$\eta = \sum_{a|T_a \in \Upsilon} s(a) \pmod{2}. \quad (\text{C12})$$

Therein,  $s(\cdot)$  is a consistent non-contextual value assignment, of which assume that it exists. Since  $A_1 A_2$  flips  $Z_2 Z_3$  under conjugation,  $s(a_{IZZ}) \longrightarrow s(a_{IZZ}) \oplus 1$ . The other values  $s$  appearing on the r.h.s. of Eq. (C12) are permuted among themselves. Therefore,  $A_1 A_2 : \eta \mapsto \eta \oplus 1$ . On the other hand,  $\eta$  is a sum of constraints (add  $2s(a_{XXX}) + 2s(a_{X_2})$  on the r.h.s.), hence must remain constant under all symmetry transformations. Contradiction. Hence, no consistent non-contextual value assignment exists.

### Appendix D: Quasi-probability functions

Here we show that the function  $\Xi : \mathcal{A} \longrightarrow \mathbb{R}$ , the collection of expectation values of interest for the  $G$ -MBQC, is a characteristic function, i.e., the Fourier transform of a quasi-probability distribution  $Q$ .

For this to hold, we impose a further consistency condition on the set  $\Omega_+$ . We require that, for all  $a, b \in \mathcal{A}$ ,

$$\mathbf{v}(a) = \mathbf{v}(b), \forall \mathbf{v} \in V \implies a = b. \quad (\text{D1})$$

This implies in particular that if  $T_a \in \Omega_+$  then  $-T_a \notin \Omega_+$ , which we had imposed initially.

For any  $a \in \mathcal{A}$ ,  $\chi(a) : V \longrightarrow \{\pm 1\}$  defined by

$$\mathbf{v} \mapsto \chi_{\mathbf{v}}(a) := (-1)^{\mathbf{v}(a)}$$

is a linear character,  $\chi_{\mathbf{u}+\mathbf{v}}(a) = \chi_{\mathbf{u}}(a)\chi_{\mathbf{v}}(a)$  for all  $a \in \mathcal{A}$ ; i.e.,  $\chi(a) \in V^*$ . If Eq. (D1) holds then all observables

$T_a \in \Omega_+$  are uniquely identifiable by the linear character  $\chi(a)$  they induce. By character orthogonality, it then holds that

$$\sum_{\mathbf{v} \in V} \bar{\chi}_{\mathbf{v}}(a) \chi_{\mathbf{v}}(b) = |V| \delta_{a,b}. \quad (\text{D2})$$

We will use this property shortly.

We now turn to the definition of the quasiprobability function  $Q$ . The domain of  $Q$  is the phase space  $V$ , Eq. (5),  $Q : V \rightarrow \mathbb{R}$ . For every phase space point  $\mathbf{v} \in V$  there is an operator  $A_{\mathbf{v}}$  such that

$$Q_{\rho}(\mathbf{v}) := \text{Tr}(A_{\mathbf{v}}\rho),$$

with

$$A_{\mathbf{v}} = \frac{1}{|V|} \sum_{a \in \mathcal{A}} (-1)^{\mathbf{v}(a)} T_a. \quad (\text{D3})$$

The characteristic function  $\Xi$  is the Fourier transform of the quasiprobability function  $Q$ ,

$$\Xi_{\rho}(a) = \sum_{\mathbf{v} \in V} (-1)^{\mathbf{v}(a)} Q_{\rho}(\mathbf{v}).$$

By Eq. (D2) it follows that

$$\Xi_{\rho}(a) = \langle T_a \rangle_{\rho}, \quad \forall a \in \mathcal{A},$$

which is how we defined  $\Xi$  in the first place.

*Example 3: One qubit.* We construct the function  $Q$  for a single qubit, based on the set

$$\Omega_+ = \{I, X, Y, Z\}.$$

The first step is to construct the phase space  $V$ . Since, for consistency, the identity  $+I$  always remains  $+I$  under all transformations in  $V$ , and there are no pairs of commuting observables in  $\Omega_+ \setminus \{I\}$ , hence no corresponding constraints, it holds that  $V \cong \mathbb{Z}_1^3$ . The eight phase point operators are thus

$$A_{\pm, \pm, \pm} = \frac{1}{8} (I \pm X \pm Y \pm Z).$$

This one-qubit quasi probability distribution has been discussed in [WB]. Note for comparison that the phase space for standard one-qubit Wigner functions has four points rather than eight.

*Example 4: GHZ-MBQC [AB].* Here, the phase space is  $V = \mathbb{Z}_2^3 \times \mathbb{Z}_2^3$  (each  $X_i$  and  $Y_i$  may be flipped individually). The corresponding quasi-probability function  $Q_{|GHZ\rangle}$  for the GHZ state is plotted in the left panel of Fig. 3. Also shown is the action of  $g_{11}$  (Eq. (4)) on  $Q_{|GHZ\rangle}$ ; See the right panel of Fig. 3. This action corresponds to a “rotation” of phase space in which the origin  $\mathbf{v} = 0$  remains fixed. This is the covariance of  $G$ , discussed below in Section D2. The effect on  $Q_{|GHZ\rangle}$  is that of a translation, by the vector  $(1, 0, 0)$  in the vertical direction (indicated by the red rectangles in Fig. 3). This situation is analogous to the symmetries of matter density in a crystal. There, the analogue of  $G$  is the point group, and the corresponding symmetry transformations are screw axes and glide planes.

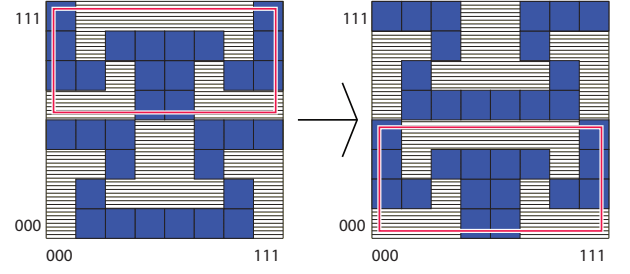


FIG. 3: Similarity transformation on the quasi-probability function  $Q_{|GHZ\rangle}$  of a GHZ-state, cf. Eq. (D3) [hatched:  $Q(\cdot) = -1/64$ , solid:  $Q(\cdot) = 3/64$ ]. The effect of the  $g \in G$  on  $Q_{|GHZ\rangle}$  are translations; i.e., the symmetry transformations of  $Q_{|GHZ\rangle}$  are analogous to screw axes and glide planes.

## 1. Basic properties of $Q$

Every quasi-probability functions  $Q$  is a linear mapping sending operators to functions on phase space  $V$ , as follows immediately from the definition. Also, probabilities for measurement outcomes of observables  $T_a \in \Omega_+$  are given by the sums of  $Q_{\rho}(\mathbf{v})$  over cosets in phase space.

Namely, the probability for obtaining the eigenvalue  $(-1)^s$  in the measurement of an observable  $T_a \in \Omega_+$  is  $p_s(a) = (1 + (-1)^s \langle T_a \rangle)/2$ . We may express  $p_s(a)$  in terms of the quasi-probability function,

$$\begin{aligned} p_s(a) &= (1 + (-1)^s \langle T_a \rangle)/2 = (1 + (-1)^s \Xi_{\rho}(a))/2 \\ &= \frac{1}{2} \sum_{\mathbf{v} \in V} (1 + (-1)^s (-1)^{\mathbf{v}(a)}) Q_{\rho}(\mathbf{v}) \\ &= \sum_{\mathbf{v} \in V} \delta_{s, \mathbf{v}(a)} Q_{\rho}(\mathbf{v}) \end{aligned}$$

The set of  $\mathbf{v} \in V$  for which  $\mathbf{v}(a) = s$  is a coset of the subspace  $V(a) = \{\mathbf{v} \in V \mid \mathbf{v}(a) = 0\}$ , as claimed. In the second line above we have used the fact that  $I \in \Omega_+$ .

## 2. Covariance of $Q$ under $G$

**Definition 1 (Covariance)** A quasi-probability function  $Q$  is covariant under a group  $\mathcal{G}$  of unitary transformations if, for all states  $\sigma$ , all phase space points  $a \in V$ , and all  $h \in H$  it holds that

$$Q_{u(h)^\dagger \sigma u(h)}(\mathbf{v}) = Q_{\sigma}(S_h \mathbf{v} + \mathbf{v}_h), \quad (\text{D4})$$

with  $S_h$  a square invertible matrix and  $\mathbf{v}_h \in V$ .

We then have the following result.

**Lemma 5** The quasi-probability function  $Q$  is covariant under the input group  $G$ . Furthermore, the origin  $\mathbf{0} \in V$  remains fixed under all  $g \in G$ , i.e.,

$$Q_{u(g)^\dagger \sigma u(g)}(\mathbf{v}) = Q_{\sigma}(S_g \mathbf{v}),$$

for all  $\mathbf{v} \in V$ , for all  $g \in G$ , and all states  $\sigma$ .

We prove Lemma 5 by way of another Lemma. We have already defined the sets  $\Omega_{\mathbf{v}} = \{(-1)^{\mathbf{v}(a)}T_a, a \in \mathcal{A}\}$ , for all  $\mathbf{v} \in V$ .  $G$  is acting on all  $T_a \in \Omega_+$  by conjugation,  $T_a \mapsto u(g)T_a u(g)^\dagger = T_{ga}$ , and this induces an action of  $G$  on the sets  $\Omega_{\mathbf{v}}$ . We define

$$g(\Omega_{\mathbf{v}}) := \{(-1)^{\mathbf{v}(a)}T_{ga}, a \in \mathcal{A}\}, \forall \mathbf{v} \in V. \quad (\text{D5})$$

We now show that this action of  $G$  permutes the sets  $\Omega_{\mathbf{v}}$ .

**Lemma 6** *For all  $g \in G, \forall \mathbf{v} \in V$ , there exists a  $g(\mathbf{v}) \in V$  such that*

$$g(\mathbf{v})(\cdot) = \mathbf{v} \circ g^{-1}(\cdot). \quad (\text{D6})$$

Then, with Eq. (D5) and Lemma 6,

$$g(\Omega_{\mathbf{v}}) = \{(-1)^{\mathbf{v}(g^{-1}a)}T_a, a \in \mathcal{A}\} = \Omega_{g(\mathbf{v})}.$$

Thus, the sets  $\Omega_{\mathbf{v}}, \mathbf{v} \in V$ , are indeed permuted by the action of  $G$ , as claimed.

*Proof of Lemma 6.* For all triples  $a, b, c \in \mathcal{A}$  with  $[T_a, T_b] = 0$  and  $T_c = (-1)^{\beta(a,b)}T_a T_b$  it holds by definition Eq. (5) of  $V$  that  $\mathbf{v}(c) = \mathbf{v}(a) + \mathbf{v}(b) \pmod{2}$ ,  $\mathbf{v} \in V$ . Hence,

$$(-1)^{\mathbf{v}(c)}T_c = (-1)^{\beta(a,b)+\mathbf{v}(a)+\mathbf{v}(b)}T_a T_b, \forall \mathbf{v} \in V. \quad (\text{D7})$$

Conjugating Eq. (D7) by any  $u(g)$ ,  $g \in G$ , we obtain, after relabeling the elements of  $\mathcal{A}$ ,

$$(-1)^{\mathbf{v}(g^{-1}c)}T_c = (-1)^{\beta(g^{-1}a, g^{-1}b)+\mathbf{v}(g^{-1}a)+\mathbf{v}(g^{-1}b)}T_a T_b, \quad (\text{D8})$$

for all  $\mathbf{v} \in V$  and all  $a, b, c \in \mathcal{A}$  with  $[T_a, T_b] = 0$  and  $T_c = (-1)^{\beta(a,b)}T_a T_b$ . Setting  $\mathbf{v} \equiv \mathbf{0}$  in Eq. (D8), it follows that,  $\forall g \in G$ ,

$$\beta(a, b) = \beta(g^{-1}a, g^{-1}b), \forall a, b \in \mathcal{A}.$$

Therefore,  $\forall g \in G, \forall \mathbf{v} \in V$  and all  $a, b, c \in \mathcal{A}$  with  $[T_a, T_b] = 0$  and  $T_c \sim T_a T_b$  it holds that

$$\mathbf{v}(g^{-1}c) = \mathbf{v}(g^{-1}a) + \mathbf{v}(g^{-1}b) \pmod{2}.$$

Thus,  $\mathbf{v} \circ g^{-1} \in V$ , for all  $\mathbf{v} \in V$  and all  $g \in G$ .  $\square$

*Proof of Lemma 5.*  $Q_{u(g)^\dagger \rho u(g)}(\mathbf{v}) = \text{Tr } u(g)A_{\mathbf{v}}u(g)^\dagger \rho$ , and we are thus interested in how the phase point operators  $A_{\mathbf{v}}$  transform under conjugation by  $g \in G$ .

$$\begin{aligned} u(g)A_{\mathbf{v}}u(g)^\dagger &= g \left( \frac{1}{|V|} \sum_{a \in \mathcal{A}} \chi_{\mathbf{v}}(a) T_a \right) g^\dagger \\ &= \frac{1}{|V|} \sum_{a \in \mathcal{A}} \chi_{\mathbf{v}}(a) T_{ga} \\ &= \frac{1}{|V|} \sum_{a \in \mathcal{A}} \chi_{\mathbf{v}}(g^{-1}a) T_a \\ &= \frac{1}{|V|} \sum_{a \in \mathcal{A}} \chi_{g(\mathbf{v})}(a) T_a \\ &= A_{g(\mathbf{v})}. \end{aligned}$$

Therein, the fourth line follows by Lemma 6. Thus, phase point operators are mapped to phase point operators by conjugation under any  $g \in G$ .

We now show that  $G$  acts linearly on  $V$ . For any  $g \in G$ , for all  $a \in \mathcal{A}$  and all  $g(\mathbf{u}), g(\mathbf{v}) \in V$ ,

$$\begin{aligned} \chi_{g(\mathbf{u})+g(\mathbf{v})}(a) &= \chi_{g(\mathbf{u})}(a) \chi_{g(\mathbf{v})}(a) \\ &= \chi_{\mathbf{u}}(g^{-1}a) \chi_{\mathbf{v}}(g^{-1}a) \\ &= \chi_{\mathbf{u}+\mathbf{v}}(g^{-1}a) \\ &= \chi_{g(\mathbf{u}+\mathbf{v})}(a). \end{aligned}$$

We may thus write  $g(\mathbf{v}) = S_g \mathbf{v}$ , for a square matrix  $S_g$ , for all  $g \in G$  and all  $\mathbf{v} \in V$ . Since  $g^{-1} \in G$ ,  $S_g$  must be invertible. Thus, Eq. (D4) holds, with the special offsets  $\mathbf{v}_g = \mathbf{0}$ , for all  $g \in G$ .  $\square$

In summary, we find that  $G$ -MBQC assumes a very particular location with respect to contextuality and covariance of quasi-probability functions. Namely,

1. The quasi-probability function  $Q$  describing the resource state  $\rho$  is covariant under the input group  $G$  (Lemma 5).
2. There is no state-independent symmetry-based contextuality proof for the pair  $(\Omega_+, G)$  (Lemma 4).
3. If the  $G$ -MBQC in question is non-trivial, then there exists a state-dependent symmetry-based contextuality proof based on the triple  $(\Omega_+, G, \rho)$  (Prop. 1).

## Appendix E: $G$ -MBQCs and group extensions

### 1. Structure of the symmetry group $E$

In our setting of  $G$ -MBQC,  $E$  is a set of symmetry transformations,

$$E = \{\eta(g)n, n \in N, g \in G\},$$

where the injection  $\eta : G \hookrightarrow E$  is defined in Eq. (16), and  $N$  is a subgroup of  $V$  with the property

$$n(a) = 0, \forall a | T_a \in \Omega_+ \setminus \mathcal{O}_+. \quad (\text{E1})$$

Here we show that (i)  $E$  is a group, (ii)  $N$  is a normal subgroup of  $E$ , and (iii)  $G \cong E/N$ . First, there is an action of  $G$  on  $N$ , namely

$$\eta(g)n = g(n)\eta(g),$$

with  $g(n) = n \circ g^{-1}$  (cf. Lemma 6 in Appendix D 2). To see this in detail, compare

$$\begin{aligned} ((\eta(g)n)(\Xi_\sigma))(a) &= (-1)^{n(a)}(\eta(g)\Xi_\sigma)(a) \\ &= (-1)^{n(a)+\Phi_g(a)}\Xi_\sigma(ga) \end{aligned}$$

with

$$\begin{aligned} ((\tilde{n}\eta(g))(\Xi_\sigma))(a) &= (-1)^{\Phi_g(a)}(\tilde{n}(\Xi_\sigma))(ga) \\ &= (-1)^{\tilde{n}(ga)+\Phi_g(a)}\Xi_\sigma(ga). \end{aligned}$$

Thus,  $n(a) = \tilde{n}(ga)$ , hence  $\tilde{n} = g(n) = n \circ g^{-1}$ , as stated above.

Multiplication of two elements of  $E$  thus yields

$$(\eta(g)n)(\eta(h)n') = \eta(g)\eta(h)h^{-1}(n)n'. \quad (\text{E2})$$

Therein, the product  $\eta(g)\eta(h)$  has yet to be specified. Since group compatibility may fail in the quantum scenario,  $\eta$  is not guaranteed to be a homomorphism. However, since all  $\eta(g)$  are symmetry transformations, it holds that

$$\eta(g)\eta(h) = \eta(gh)\lambda(g,h), \quad \forall g,h \in G, \quad (\text{E3})$$

where  $\lambda : G \times G \rightarrow N$ .

From the above, the product of two elements in  $E$  is

$$(\eta(g)n)(\eta(h)n') = \eta(gh)(\lambda(g,h)h^{-1}(n)n'), \quad (\text{E4})$$

which is again of form  $\eta(\tilde{g})\tilde{n}$ , where  $\tilde{n} \in N$  and  $\tilde{g} \in G$ .  $E$  is thus a group.

Further, with Eq. (E2),  $\eta(g)n\eta(g)^{-1} = g(n)$ , for all  $g \in G$ . If  $n \in N$  preserves  $\Xi_\rho$ , then so does  $\eta(g)n\eta(g)^{-1} \in V$ , and therefore  $g(n) \in N$ . Thus,  $N$  is a normal subgroup of  $E$ . Finally, with Eq. (E4),  $G = E/N$ .

## 2. Classification

The function  $\lambda$  appearing in Eq. (E3) measures the indeterminacy of the group  $E$  given its normal subgroup  $N$  and its quotient  $G \cong E/N$ . However, by Eq. (16),  $\lambda$  is specified if the phase function  $\Phi$  is,

$$\lambda(g,h)(a) = \Phi_h(a) + \Phi_g(ha) - \Phi_{gh}(a) \mod 2. \quad (\text{E5})$$

Therein, we have used the convention that  $(\Phi_g(\Xi))(a) = (-1)^{\Phi_g(a)}\Xi(a)$ .

Now, the function  $\lambda$  is subject to a constraint and an identification. The constraint arises from the associativity of multiplication in  $G$ , namely  $\eta(ghk) = \eta((gh)k) = \eta(g(hk))$ ,  $\forall g,h,k \in G$ . By Eq. (E3) this leads to a condition on  $\lambda$ , which in its topological formulation reads

$$d\lambda = 0. \quad (\text{E6})$$

The identification arises from the transformations

$$\Phi_g \rightarrow \Phi'_g = \Phi_g + n_g \mod 2, \quad \forall g \in G,$$

where  $n_g \in N$ . Clearly these are symmetry transformations: The offsets  $n_g$  in the phase functions do, by Eq. (E1), neither affect the resource state  $\rho$  nor the outputted function  $o : G \rightarrow \mathbb{Z}_2$ . The effect of these equivalence transformations on  $\lambda$  is

$$\lambda \rightarrow \lambda + dn \mod 2. \quad (\text{E7})$$

With the constraint Eq. (E6) and identification Eq. (E7), the equivalence classes  $[\lambda]$  of the functions  $\lambda$  are labeled by the elements of  $H^2(G, N)$ .

For any fixed function  $\lambda$ , the phase function  $\Phi$  is determined up to an offset  $\Phi_0$ , with  $d\Phi_0 \equiv 0$ , cf. Eq. (E5). Now denote by  $o, o', \delta o : G \rightarrow \mathbb{Z}_2$  the output functions resulting from the phase functions  $\Phi$ ,  $\Phi + \Phi_0$  and  $\Phi_0$ , respectively. Then, by Eq. (7),

$$o' = o + \delta o \mod 2.$$

By Proposition 2,  $\delta o$  is computationally trivial, and all  $G$ -MBQCs resulting from a given  $[\lambda]$  are thus equivalent in complexity. Thus, for any given  $G$  and  $\mathcal{O}_+$  (hence  $N$ ), the corresponding  $G$ -MBQCs are classified by  $H^2(G, N)$ .

---

[AB] J. Anders and D.E. Browne, Phys. Rev. Lett. **102**, 050502 (2009).  
[DM] N. D. Mermin, Rev. Mod. Phys. **65**, 803 (1993).  
[JL] J. Lawrence, Phys. Rev. A **89**, 012105 (2014).  
[LS] P. Lisonek, R. Raussendorf and V. Singh, arXiv:1401.3035.

[RB] R. Raussendorf and H.J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).  
[WB] J.J. Wallman, S.D. Bartlett, Phys. Rev. A **85**, 062121 (2012).